Abstract

An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorised party or entity to a computer system or network, the intrusion detection system comprising means for monitoring the activity relative to the computer system or network, means for receiving and storing one or more general rules, each of the general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion, and matching means for receiving data relating to activity relative to said computer system or network from the monitoring means and for comparing, in a semantic manner, sets of actions forming the activity against the one or more general rules to identify an intrusion or attempted intrusion. Inductive logic techniques are proposed for suggesting new intrusion detection rules for inclusion into the system, based on examples of sinister traffic.